LES MENACES PERSISTANTES AVANCÉES EN CYBERSÉCURITÉ
LA GUERRE CYBERNÉTIQUE

Nicolae Sfetcu



MultiMedia Publishing

Les menaces persistantes avancées en cybersécurité – La guerre cybernétique

APERÇU DU LIVRE

Menaces persistantes avancées

Nicolae SFETCU
nicolae@sfetcu.com[1]

Sfetcu, Nicolae (2024), *Les menaces persistantes avancées en cybersécurité – La guerre cybernétique*, MultiMedia Publishing, ISBN 978-606-033-868-0, DOI: 10.58679/MM35522, https://www.telework.ro/fr/e-books/les-menaces-persistantes-avancees-en-cybersecurite-la-guerre-cybernetique/

[1] Chercheur - Académie Roumaine - Comité Roumain pour l''Histoire et la Philosophie des Sciences et des Techniques (CRIFST), Division Histoire des Sciences (DIS), ORCID : 0000-0002-0162-9973

Table des matières

Les menaces persistantes avancées en cybersécurité – La guerre cybernétique

Nicolae SFETCU

Advanced Persistent Threats in Cybersecurity – Cyber Warfare

Abstract

This book aims to provide a comprehensive analysis of Advanced Persistent Threats (APTs), including their characteristics, origins, methods, consequences, and defense strategies, with a focus on detecting these threats. It explores the concept of advanced persistent threats in the context of cyber security and cyber warfare. APTs represent one of the most insidious and challenging forms of cyber threats, characterized by their sophistication, persistence, and targeted nature. The paper examines the origins, characteristics and methods used by APT actors. It also explores the complexities associated with APT detection, analyzing the evolving tactics used by threat actors and the corresponding advances in detection methodologies. It highlights the importance of a multi-faceted approach that integrates technological innovations with proactive defense strategies to effectively identify and mitigate APT.
Keywords: Advanced Persistent Threats, APT, cybersecurity, cyber warfare, threat detection, cyberattack

Résumé

Cet ouvrage vise à fournir une analyse complète des menaces persistantes avancées (APT), y compris leurs caractéristiques, origines, méthodes, conséquences et stratégies de défense, en mettant l'accent sur la détection de ces menaces. Il explore le concept de menaces persistantes avancées dans le contexte de la cybersécurité et de la cyberguerre. Les APT représentent l'une des formes de cybermenaces les plus insidieuses et les plus complexes, caractérisée par leur sophistication, leur persistance et leur nature ciblée. L'article examine les origines, les caractéristiques et les méthodes utilisées par les acteurs de l'APT. Il explore également les complexités associées à la détection des APT, en analysant l'évolution des tactiques utilisées par les acteurs de la menace et les avancées correspondantes dans les méthodologies de détection. Il souligne l'importance d'une approche multidimensionnelle intégrant les innovations technologiques à des stratégies de défense proactives pour identifier et atténuer efficacement les APT.
Mots-clés : menaces persistantes avancées, APT, cybersécurité, guerre cybernétique, détection des menaces, cyberattaque

Menaces persistantes avancées

Les menaces persistantes avancées (Advanced Persistent Threats, APT) sont une classe de cybermenaces qui posent un défi important aux organisations et aux nations du monde entier. Ils

sont connus pour leurs tactiques, techniques et procédures avancées, ainsi que pour leur capacité à s'infiltrer et à opérer de manière persistante sur les systèmes cibles pendant de longues périodes.

Les APT sont généralement coordonnées par un État ou un groupe parrainé par l'État (Kaspersky 2023b) (Cisco 2023). Les motivations de ces acteurs menaçants sont généralement l'espionnage militaire, géopolitique ou économique (Cole 2013). Ces secteurs ciblés comprennent le gouvernement, la défense, les services financiers, les services juridiques, l'industrie, les télécommunications, les biens de consommation, etc. (FireEye 2019).

Le « temps de contact » moyen, pendant lequel une attaque APT n'est pas détectée, était en moyenne de 71 jours en Amérique du Nord, de 177 jours dans la région EMEA et de 204 jours dans la région APAC en 2018 (Mandiant 2021).

Les menaces persistantes avancées combinent diverses formes d'attaque, de l'ingénierie sociale aux exploits techniques. Les APT utilisent généralement des vecteurs d'espionnage traditionnels (Ghafir et Prenosil 2014), notamment l'ingénierie sociale, l'intelligence humaine et l'infiltration, pour attaquer le réseau en installant des logiciels malveillants personnalisés (logiciels malveillants) (Symantec 2018b). La diversité et la furtivité des APT en font un enjeu central en matière de cybersécurité en raison de la nature asymétrique des attaques, se tournant souvent vers la théorie des jeux pour modéliser les conflits en utilisant les jeux matriciels comme outil d'atténuation des risques. Les modèles APT de la théorie des jeux peuvent être dérivés directement de l'analyse topologique de la vulnérabilité, ainsi que des évaluations des risques, conformément aux normes courantes de gestion des risques telles que la famille ISO 31000 (Rass, König, et Schauer 2017).

L'hétérogénéité, la connectivité et l'ouverture croissantes des systèmes d'information permettent d'accéder à un système par plusieurs chemins différents. Pour garantir la sécurité, des outils et techniques semi-automatisés sont utilisés pour détecter et atténuer les vulnérabilités, mais ces attaques s'adaptent rapidement à ces configurations afin qu'elles restent « sous le radar ». Les contre-mesures ont une latence plus élevée, étant inefficaces en cas de changements soudains dans les stratégies d'attaque d'un adversaire invisible (Rass, König, et Schauer 2017).

Les menaces persistantes avancées sont apparues comme une version nouvelle et complexe des attaques multi-étapes (MSA) (Kyriakopoulos et al. 2018), tandis que les systèmes de détection APT actuels se concentrent davantage sur l'émergence d'alertes de détection que sur la prévision des menaces (Ghafir et al. 2019). La prévision des étapes APT révèle non seulement le cycle de

vie APT à ses débuts, mais aide également à comprendre les stratégies et les objectifs de l'attaquant. De plus, l'Internet des objets (IoT) fait des appareils connectés à Internet des cibles faciles pour les cyberattaques (Ghafir, Kyriakopoulos, et al. 2018). Le coût mondial de la cybercriminalité a atteint 600 milliards de dollars en 2018, selon un rapport de McAfee (McAfee 2018).

Pour contrer les cyberattaques, les analystes utilisent généralement des systèmes de détection d'intrusion (IDS) en faisant correspondre les modèles d'attaque connus (basés sur les signatures) en comparant les données à une base de données contenant une liste de signatures d'attaque connues), ou en observant des anomalies (écart par rapport à un profil de référence) (Santoro et al. 2017). L'objectif visé d'APT est l'espionnage et l'exfiltration de données. L'attaque peut durer des semaines ou des années, avec de très longues périodes entre les étapes de l'attaque, ce qui rend difficile la détection en corrélant plusieurs alertes au cours du cycle de vie de l'APT (Mandiant 2013). Les méthodes traditionnelles de correspondance de modèles sont inefficaces dans le cas des APT, car il n'y a pas de modèle d'ordre et de fréquences entre les étapes, en raison des limitations techniques des mécanismes statiques de l'institution attaquée ou de l'utilisation par l'attaquant de techniques nouvelles et dynamiques. Une APT se déroule en plusieurs étapes, les privilèges, informations et ressources de l'attaquant s'accumulant à chaque étape.

Dans 76 % des organisations touchées par les APT, les logiciels antivirus et les systèmes de détection des menaces étaient inefficaces. Lors de la conférence Infosecurity Europe 2011, les APT ont été classées parmi les plus grandes cybermenaces du monde moderne (Rot et Olszewski 2017). Selon un rapport de Deloitte (Deloitte 2016), les facteurs clés dans la lutte contre les APT sont : une évaluation constante des risques, une sécurité offensive et la formation du personnel (Rot 2009).

Définition de l'APT

Une cyberattaque courante vise à exploiter des vulnérabilités pour voler des données aux entreprises (P. Chen, Desmet, et Huygens 2014), provoquant ainsi des dommages non critiques. Une APT dispose de bien plus de ressources et se concentre sur les grandes organisations et les institutions gouvernementales, causant des dommages graves, voire critiques.

Beaucoup pensent que le terme APT est surchargé parce que différentes personnes l'appellent différemment. La définition donnée par le National Institute of Standards and Technology (NIST) des États-Unis indique qu'un APT est (NIST 2011) :

« Un adversaire qui possède des niveaux d'expertise sophistiqués et des ressources importantes qui lui permettent de créer des opportunités pour atteindre ses objectifs en utilisant plusieurs vecteurs d'attaque (par exemple, cyber, physique et tromperie). Ces objectifs comprennent généralement l'établissement et l'extension de la présence au sein de l'infrastructure informatique des organisations ciblées dans le but d'exfiltrer des informations, de saper ou d'entraver les aspects critiques d'une mission, d'un programme ou d'une organisation ; ou se positionner pour réaliser ces objectifs à l'avenir. La menace persistante avancée : (i) poursuit ses objectifs de manière répétée sur une période de temps prolongée ; (ii) s'adapte aux efforts des défenseurs pour y résister ; et (iii) est déterminé à maintenir le niveau d'interaction nécessaire pour exécuter ses objectifs. »

Les principales caractéristiques d'une APT découlent de son nom lui-même :

- **Menace** – Les APT ont à la fois des capacités et des intentions, et sont exécutées par le biais d'actions coordonnées, avec un personnel qualifié, motivé, organisé et bien financé (Maloney 2018) (IT Governance 2023).
- **Persistance** – Les attaquants utilisent une approche « faible et lente » dans le cadre d'une stratégie cohérente ; s'ils perdent l'accès à leur cible, ils tenteront à nouveau de l'obtenir. Leurs objectifs sont de maintenir un accès à long terme (IT Governance 2023) (Arntz 2016).
- **Avancé** – Les attaquants disposent d'un large éventail de techniques et d'outils de pointe, certains même innovants, et peuvent inclure des composants couramment disponibles. Ils tentent généralement d'établir plusieurs points d'entrée dans les réseaux ciblés et combinent plusieurs méthodes, outils et techniques pour atteindre leurs objectifs, maintenir l'accès et compromettre la cible (Maloney 2018) (Arntz 2016).

La spécificité des APT leur permet de conserver l'accès même si une activité malveillante est découverte et qu'une réponse à l'incident est déclenchée, permettant aux défenseurs de la cybersécurité de clôturer un compromis.

Histoire de l'APT

Les attaques contre la cybersécurité via des courriers électroniques ciblés, combinées à l'ingénierie sociale et à l'utilisation de chevaux de Troie pour exfiltrer des informations, ont été utilisées dès le début des années 1990 et ont été rendues publiques par les CERT britanniques et américains en 2005. Le terme « advanced persistent threats » a été utilisé pour la première fois dans le United States Air Force en 2006 (SANS 2013), par le colonel Greg Rattray (Holland 2013).

À travers le projet Stuxnet, les États-Unis ont ciblé le matériel informatique du programme nucléaire iranien, un exemple d'attaque APT (Virvilis et Gritzalis 2013).

PC World a signalé une augmentation de 81 % des APT entre 2010 et 2011. Plusieurs pays ont utilisé le cyberespace pour collecter des informations via les APT (Grow, Epstein, et Tschang

2008), par l'intermédiaire de groupes affiliés ou d'agents de gouvernements d'États souverains (Daly 2009).

Une étude de Bell Canada a révélé une présence généralisée des APT au sein du gouvernement canadien et des infrastructures critiques, avec des attaques attribuées à des acteurs chinois et russes (McMahon et Rohozinski 2013).

Google, Adobe Systems, Juniper Networks et Symantec ont été victimes d'une attaque APT appelée Operation Aurora (Matthews 2019).

Plusieurs attaques dans les secteurs militaire, financier, énergétique, nucléaire, éducatif, aérospatial, des télécommunications, chimique et gouvernemental ont été signalées en 2011 (Y. Wang et al. 2016). Les attaques APT les plus médiatisées incluent Stuxnet, RAS Breach, Operation Aurora, Duqu, Operation Ke3chang, Flame, Snow Man, Red October et Mini duke, avec des attaques de logiciels malveillants plus récentes Ratankba, ActiveX, etc. (Xu et al. 2015). Leurs objectifs habituels sont le cyber espionnage ayant des intérêts de sécurité nationale et le sabotage des infrastructures stratégiques. Les attaques utilisent des dispositifs matériels et des outils logiciels, avec une approche systématique qui s'appuie souvent sur l'ingénierie sociale comme principal mécanisme d'accès et d'exploits zero-day (Adelaiye, Ajibola, et Silas 2019).

Industroyer, un logiciel malveillant découvert en 2016, a ciblé le réseau électrique de la capitale ukrainienne, provoquant une panne de courant à court terme dans cette zone (Tollefson 2020).

Caractéristiques de l'APT

Les menaces persistantes avancées se caractérisent par la persistance (restant non détectées dans un environnement cible pendant de longues périodes, parfois même des années), un ciblage précis (sélectif, adaptant leurs attaques aux vulnérabilités ou aux faiblesses des cibles) et la sophistication (génération de techniques avancées et de pointe, certaines même innovantes, utilisant souvent des exploits zero-day, de l'ingénierie sociale et d'autres méthodes sophistiquées).

Les caractéristiques distinctives de l'APT sont (P. Chen, Desmet, et Huygens 2014):

Cibles spécifiques et objectifs clairs. Les cibles des attaques APT sont spécifiques, généralement des gouvernements, des organisations ou des armées de pays, ce qui limite leur portée d'attaque. Leur objectif est principalement d'obtenir des avantages stratégiques en matière de sécurité nationale et d'obtention d'informations secrètes.

Attaquants experts, organisés et ingénieux. Les attaquants sont généralement des pirates informatiques qualifiés travaillant de manière coordonnée, employés dans une cyber-unité gouvernementale/militaire (Mandiant 2013) ou des cyber mercenaires, prêts à opérer pendant de longues périodes et à exploiter des vulnérabilités zero-day. Parfois, ils peuvent même opérer avec le soutien des services militaires ou de renseignement de l'État.

Attaques à long terme et, si nécessaire, tentatives répétées. Les campagnes APT passent inaperçues pendant des mois ou des années. Les acteurs de l'APT adaptent constamment leurs efforts aux conditions changeantes ou pour surmonter une difficulté particulière.

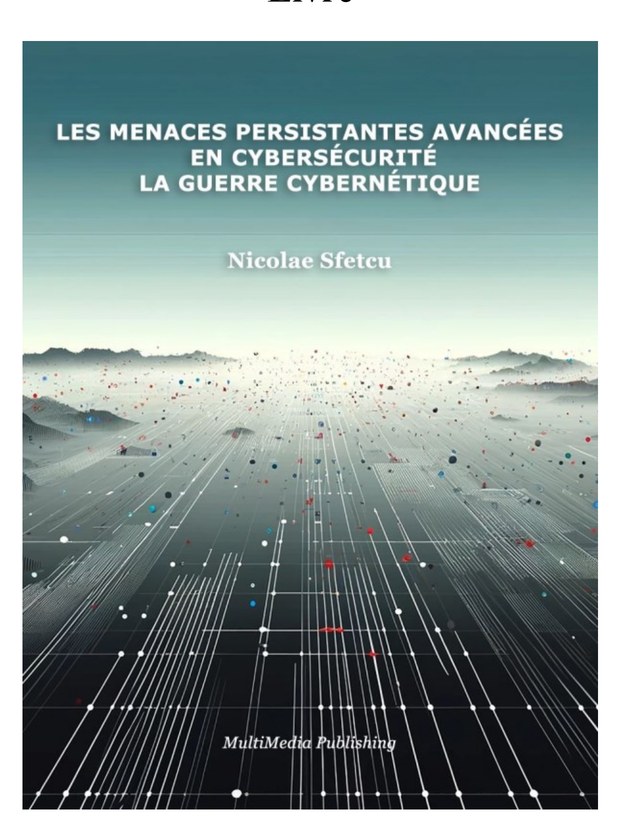
Techniques furtives et évasives. Les attaques APT peuvent passer inaperçues, se cacher dans le trafic réseau et interagir de manière minimale, uniquement pour atteindre des objectifs définis. Ils peuvent utiliser des exploits zero-day pour éviter la détection basée sur les signatures et le chiffrement pour usurper le trafic réseau.

	Attaques traditionnelles	**Attaques APT**
Agresseur	Personne principalement seule	Groupe très organisé, sophistiqué, déterminé et doté de ressources suffisantes
Cible	Non précisée, principalement systèmes individuelles	Organisations spécifiques, institutions gouvernementales, entreprises commerciales
Objectif	Avantages financiers, démonstration de capacités	Avantages compétitifs, avantages stratégiques
Approche	Course unique, « briser et saisir », courte période	Tentatives répétées, reste bas et lent, s'adapte pour résister aux défenses, long terme

Tableau 1 : Comparaison des attaques traditionnelles et APT. Source (P. Chen, Desmet, et Huygens 2014)

Table des matières

Livre



Ce livre vise à fournir une analyse complète des menaces persistantes avancées, y compris leurs caractéristiques, origines, méthodes, conséquences et stratégies de défense, en mettant l'accent sur la détection de ces menaces. Il explore le concept de menaces persistantes avancées dans le contexte de la cybersécurité et de la cyberguerre. Les menaces persistantes avancées représentent l'une des formes de cybermenaces les plus insidieuses et les plus complexes, caractérisée par leur sophistication, leur persistance et leur nature ciblée. Le livre examine les origines, les caractéristiques et les méthodes utilisées par les acteurs des menaces persistantes

avancées. Il explore également les complexités associées à la détection des menaces persistantes avancées, en analysant l'évolution des tactiques utilisées par les acteurs de la menace et les avancées correspondantes dans les méthodologies de détection. Il souligne l'importance d'une approche multidimensionnelle intégrant les innovations technologiques à des stratégies de défense proactives pour identifier et atténuer efficacement les menaces persistantes avancées.

MultiMedia Publishing https://www.telework.ro/fr/e-books/les-menaces-persistantes-avancees-en-cybersecurite-la-guerre-cybernetique/

Digital: EPUB (ISBN 978-606-033-866-6), Kindle (ISBN 978-606-033-867-3) PDF (ISBN 978-606-033-868-0)

DOI: 10.58679/MM35522

Date de publication: 16.07.2024

Bibliographie

Adams, Chris. 2018. « Learning the lessons of WannaCry ». *Computer Fraud & Security* 2018 (9): 6-9. https://doi.org/10.1016/S1361-3723(18)30084-8.

Adelaiye, Oluwasegun, Aminat Ajibola, et Faki Silas. 2019. « Evaluating Advanced Persistent Threats Mitigation Effects: A Review », février.

Aleroud, Ahmed, et Lina Zhou. 2017. « Phishing environments, techniques, and countermeasures: A survey ». *Computers & Security* 68 (juillet):160-96. https://doi.org/10.1016/j.cose.2017.04.006.

Alperovitch, Dmitri. 2011. « Revealed: Operation Shady RAT - McAfee ». https://icscsi.org/library/Documents/Cyber_Events/McAfee%20-%20Operation%20Shady%20RAT.pdf.

Al-Saraireh, Jaafer, et Ala' Masarweh. 2022. « A novel approach for detecting advanced persistent threats ». *Egyptian Informatics Journal* 23 (4): 45-55. https://doi.org/10.1016/j.eij.2022.06.005.

Alshamrani, Adel, Sowmya Myneni, Ankur Chowdhary, et Dijiang Huang. 2019. « A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities ». *IEEE Communications Surveys & Tutorials* 21 (2): 1851-77. https://doi.org/10.1109/COMST.2019.2891891.

Al-Yaseen, Wathiq Laftah, Zulaiha Ali Othman, et Mohd Zakree Ahmad Nazri. 2017. « Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system ». *Expert Systems with Applications* 67 (janvier):296-303. https://doi.org/10.1016/j.eswa.2016.09.041.

Amouri, Amar, Vishwa T. Alaparthy, et Salvatore D. Morgera. 2020. « A Machine Learning Based Intrusion Detection System for Mobile Internet of Things ». *Sensors* 20 (2): 461. https://doi.org/10.3390/s20020461.

Apruzzese, Giovanni, Fabio Pierazzi, Michele Colajanni, et Mirco Marchetti. 2017. « Detection and Threat Prioritization of Pivoting Attacks in Large Networks ». *IEEE Transactions on*

Emerging Topics in Computing PP (octobre):1-1. https://doi.org/10.1109/TETC.2017.2764885.

Arachchilage, Nalin, et Steve Love. 2014. « Security awareness of computer users: A phishing threat avoidance perspective ». *Computers in Human Behavior* 38 (septembre):304-12. https://doi.org/10.1016/j.chb.2014.05.046.

Arntz, Pieter. 2016. « Explained: Advanced Persistent Threat (APT) | Malwarebytes Labs ». Malwarebytes. 25 juillet 2016. https://www.malwarebytes.com/blog/news/2016/07/explained-advanced-persistent-threat-apt/.

Ashford, Warwick. 2011. « How to Combat Advanced Persistent Threats: APT Strategies to Protect Your Organisation | Computer Weekly ». ComputerWeekly.Com. 2011. https://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation.

Ask, M. 2013. « Advanced Persistent Threat (APT) Beyond the hype Project report in IMT 4582 Network security at Gjøvik University College during spring 2013 ». In . https://www.semanticscholar.org/paper/Advanced-Persistent-Threat-(-APT-)-Beyond-the-hype-Ask/a140cd962b136474685db82de60bb15f4fe1d7e1.

Axelsson, Stefan. 2000. « The base-rate fallacy and the difficulty of intrusion detection ». *ACM Transactions on Information and System Security* 3 (3): 186-205. https://doi.org/10.1145/357830.357849.

Azaria, Amos, Ariella Richardson, Sarit Kraus, et V. Subrahmanian. 2014. « Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data ». *IEEE Transactions on Computational Social Systems* 1 (juin):135-55. https://doi.org/10.1109/TCSS.2014.2377811.

Bai, Tim, Haibo Bian, Abbas Abou Daya, Mohammad Salahuddin, Noura Limam, et Raouf Boutaba. 2019. *A Machine Learning Approach for RDP-based Lateral Movement Detection*. https://doi.org/10.1109/LCN44214.2019.8990853.

Balduzzi, Marco, Vincenzo Ciangaglini, et Robert McArdle. 2013. *Targeted attacks detection with SPuNge*. https://doi.org/10.1109/PST.2013.6596053.

BBC. 2009. « Major Cyber Spy Network Uncovered », 29 mars 2009. http://news.bbc.co.uk/2/hi/americas/7970471.stm.

Bencsáth, B., Gábor Pék, L. Buttyán, et M. Félegyházi. 2012. « Duqu: Analysis, Detection, and Lessons Learned ». In . https://www.semanticscholar.org/paper/Duqu%3A-Analysis%2C-Detection%2C-and-Lessons-Learned-Bencs%C3%A1th-P%C3%A9k/9974cdf65ffbdee47837574432b0f8b59ffbddd1.

Benjamin, Victor, Weifeng Li, et Thomas Holt. 2015. *Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops*. https://doi.org/10.1109/ISI.2015.7165944.

Bere, Mercy, Fungai Bhunu Shava, Attlee Gamundani, et Isaac Nhamu. 2015. « How Advanced Persistent Threats Exploit Humans ». *IJCSI*, novembre.

Bertino, Elisa, et Gabriel Ghinita. 2011. « Towards Mechanisms for Detection and Prevention of Data Exfiltration by Insiders: Keynote Talk Paper ». In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 10-19. Hong Kong China: ACM. https://doi.org/10.1145/1966913.1966916.

Bhatt, Parth, Edgar Toshiro Yano, et Per Gustavsson. 2014. « Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks ». In *2014 IEEE 8th International*

Symposium on Service Oriented System Engineering, 390-95. https://doi.org/10.1109/SOSE.2014.53.

Bowen, Brian M., Shlomo Hershkop, Angelos D. Keromytis, et Salvatore J. Stolfo. 2009. « Baiting Inside Attackers Using Decoy Documents ». In *Security and Privacy in Communication Networks*, édité par Yan Chen, Tassos D. Dimitriou, et Jianying Zhou, 51-70. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-05284-2_4.

Brewer, Ross. 2014. « Advanced persistent threats: Minimising the damage ». *Network Security* 2014 (avril):5-9. https://doi.org/10.1016/S1353-4858(14)70040-6.

Bro, Rasmus, et Age K. Smilde. 2014. « Principal Component Analysis ». *Analytical Methods* 6 (9): 2812-31. https://doi.org/10.1039/C3AY41907J.

Brogi, Guillaume, et Elena Di Bernardino. 2019. « Hidden Markov models for advanced persistent threats ». *International Journal of Security and Networks* 14 (4): 181. https://doi.org/10.1504/IJSN.2019.103147.

Brogi, Guillaume, et Valerie Viet Triem Tong. 2016. « TerminAPTor: Highlighting Advanced Persistent Threats through Information Flow Tracking ». *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, novembre, 1-5. https://doi.org/10.1109/NTMS.2016.7792480.

Bulgurcu, Burcu, Hasan Cavusoglu, et Izak Benbasat. 2010. « Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness ». *MIS Quarterly* 34 (3): 523-48. https://doi.org/10.2307/25750690.

Busby, J. S., B. S. S. Onggo, et Y. Liu. 2016. « Agent-based computational modelling of social risk responses ». *European Journal of Operational Research* 251 (3): 1029-42. https://doi.org/10.1016/j.ejor.2015.12.034.

Chaitanya, Krishna T., HariGopal Ponnapalli, Dylan Herts, et Juan Pablo. 2012. « Analysis and Detection of Modern Spam Techniques on Social Networking Sites ». *2012 Third International Conference on Services in Emerging Markets*, décembre, 147-52. https://doi.org/10.1109/ICSEM.2012.28.

Chandola, Varun, Arindam Banerjee, et Vipin Kumar. 2009. « Anomaly Detection: A Survey ». *ACM Comput. Surv.* 41 (juillet). https://doi.org/10.1145/1541880.1541882.

Chandra Jadala, Dr, Challa Narasimham, et Sai Kiran Pasupuleti. 2020. « Detection of Deceptive Phishing Based on Machine Learning Techniques ». In , 13-22. https://doi.org/10.1007/978-981-15-2407-3_2.

Chen, Ping, Lieven Desmet, et Christophe Huygens. 2014. « A Study on Advanced Persistent Threats ». In *Communications and Multimedia Security*, édité par Bart De Decker et André Zúquete, 63-72. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-44885-4_5.

Chen, Zhiyan, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, H.T. Mouftah, et Petar Djukic. 2022. « Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats ». *ACM Computing Surveys* 55 (avril). https://doi.org/10.1145/3530812.

Chu, Wen-Lin, Chih-Jer Lin, et Ke-Neng Chang. 2019. « Detection and Classification of Advanced Persistent Threats and Attacks Using the Support Vector Machine ». *Applied Sciences* 9 (21): 4579. https://doi.org/10.3390/app9214579.

Cisco. 2023. « What Is an Advanced Persistent Threat (APT)? » Cisco. 2023. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.

CloudStrike. 2023. « Cyber Attacks on SMBs: Current Stats and How to Prevent Them ». Crowdstrike.Com. 2023. https://www.crowdstrike.com/solutions/small-business/cyber-attacks-on-smbs/.

Cobb, Michael. 2013. « The Evolution of Threat Detection and Management ». https://docs.media.bitpipe.com/io_10x/io_109837/item_691345/EMC_sSecurity_IO%23109837_E-Guide_060513.pdf.

Cobb, Stephen. 1996. *The NCSA Guide to PC and LAN Security*. McGraw-Hill.

Cole, Eric. 2013. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Syngress.

Conti, Mauro, Luigi V. Mancini, Riccardo Spolaor, et Nino Vincenzo Verde. 2015. « Can't You Hear Me Knocking: Identification of User Actions on Android Apps via Traffic Analysis ». In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 297-304. CODASPY '15. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2699026.2699119.

Coppolino, L., Michael Jäger, Nicolai Kuntze, et Roland Rieke. 2012. « A Trusted Information Agent for Security Information and Event Management ». In , 6-12.

Crouse, Michael, Bryan Prosser, et Errin Fulp. 2015. *Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses*. https://doi.org/10.1145/2808475.2808480.

CSS. 2019. « Trend Analysis - The Israeli Unit 8200 An OSINT-based study ». CSS CYBER DEFENSE PROJECT. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf.

Daly, Michael K. 2009. « The Advanced Persistent Threat (or Informa5onized Force Opera5ons) ». https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf.

De Vries, Johannes, Hans Hoogstraaten, Jan Van Den Berg, et Semir Daskapan. 2012. « Systems for Detecting Advanced Persistent Threats: A Development Roadmap Using Intelligent Data Analysis ». *2012 International Conference on Cyber Security*, décembre, 54-61. https://doi.org/10.1109/CyberSecurity.2012.14.

Deloitte. 2016. « Cyber Espionage - The harsh reality of advanced security threats ». https://indianstrategicknowledgeonline.com/web/us_aers_cyber_espionage_07292011.pdf.

Denault, Michel, Dimitris Karagiannis, Dimitris Gritzalis, et Paul Spirakis. 1994. « Intrusion detection: Approach and performance issues of the SECURENET system ». *Computers & Security* 13 (6): 495-508. https://doi.org/10.1016/0167-4048(91)90138-4.

Denning, D.E. 1987. « An Intrusion-Detection Model ». *IEEE Transactions on Software Engineering* SE-13 (2): 222-32. https://doi.org/10.1109/TSE.1987.232894.

Dijk, Marten van, Ari Juels, Alina Oprea, et Ronald L. Rivest. 2013. « FlipIt: The Game of "Stealthy Takeover" ». *Journal of Cryptology* 26 (4): 655-713. https://doi.org/10.1007/s00145-012-9134-5.

EC-Council. 2023. « What Is Cyber Threat Modeling | Importance of Threat Modeling ». *EC-Council* (blog). 2023. https://www.eccouncil.org/threat-modeling/.

Edwards, Benjamin, Tyler Moore, George Stelle, Steven Hofmeyr, et Stephanie Forrest. 2012. « Beyond the Blacklist: Modeling Malware Spread and the Effect of Interventions ». *Proceedings New Security Paradigms Workshop*, février. https://doi.org/10.1145/2413296.2413302.

Eke, Hope Nkiruka, Andrei Petrovski, et Hatem Ahriz. 2019. « The use of machine learning algorithms for detecting advanced persistent threats ». In *Proceedings of the 12th International Conference on Security of Information and Networks*, 1-8. SIN '19. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3357613.3357618.

ETDA. 2023. « Threat Group Cards: A Threat Actor Encyclopedia ». 2023. https://apt.etda.or.th/cgi-bin/aptgroups.cgi.

Falliere, Nicolas, Liam O Murchu, et Eric Chien. 2011. « W32.Stuxnet Dossier ». Symantec. https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf.

Feily, Maryam, Alireza Shahrestani, et Sureswaran Ramadass. 2009. « A Survey of Botnet and Botnet Detection ». *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, 268-73. https://doi.org/10.1109/SECURWARE.2009.48.

Ferrer, Zarestel, et Methusela Cebrian Ferrer. 2010. « In-depth Analysis of Hydraq - The face of cyberwar enemies unfolds ». http://cybercampaigns.net/wp-content/uploads/2013/05/Hydraq.pdf.

FireEye. 2019. « Cyber Threats to the Financial Services and Insurance Industries ». https://web.archive.org/web/20190811091624/https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/ib-finance.pdf.

Fortinet. 2023. « What Is a Watering Hole Attack? » Fortinet. 2023. https://www.fortinet.com/resources/cyberglossary/watering-hole-attack.

Friedberg, Ivo, et Roman Fiedler. 2014. « Dealing with Advanced Persistent Threats in Smart Grid ICT Networks: 5th IEEE Innovative Smart Grid Technologies Conference ». Édité par Florian Skopik. *Proceedings of the 5th IEEE Innovative Smart Grid Technologies Conference*, 1-6.

Friedberg, Ivo, Florian Skopik, Giuseppe Settanni, et Roman Fiedler. 2015. « Combating advanced persistent threats: From network event correlation to incident detection ». *Computers & Security* 48 (février):35-57. https://doi.org/10.1016/j.cose.2014.09.006.

García-Teodoro, Pedro, Jesús Díaz-Verdejo, Gabriel Maciá-Fernández, et Enrique Vázquez. 2009. « Anomaly-based network intrusion detection: Techniques, systems and challenges ». *Computers & Security* 28 (février):18-28. https://doi.org/10.1016/j.cose.2008.08.003.

Ghafir, Ibrahim, Mohammad Hammoudeh, Vaclav Prenosil, Liangxiu Han, Robert Hegarty, Khaled Rabie, et Francisco J. Aparicio-Navarro. 2018. « Detection of advanced persistent threat using machine-learning correlation analysis ». *Future Generation Computer Systems* 89 (décembre):349-59. https://doi.org/10.1016/j.future.2018.06.055.

Ghafir, Ibrahim, Konstantinos Kyriakopoulos, Francisco Aparicio-Navarro, S. Lambotharan, Basil AsSadhan, et Hamad BinSalleeh. 2018. « A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection ». *IEEE Access* PP (juillet):40008-23. https://doi.org/10.1109/ACCESS.2018.2855078.

Ghafir, Ibrahim, Konstantinos G. Kyriakopoulos, Sangarapillai Lambotharan, Francisco J. Aparicio-Navarro, Basil Assadhan, Hamad Binsalleeh, et Diab M. Diab. 2019. « Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats ». *IEEE Access* 7:99508-20. https://doi.org/10.1109/ACCESS.2019.2930200.

Ghafir, Ibrahim, et Vaclav Prenosil. 2014. « Advanced Persistent Threat Attack Detection: An Overview ». *International Journal Of Advances In Computer Networks And Its Security*, décembre, 154.

———. 2016. « Proposed Approach for Targeted Attacks Detection ». In *Advanced Computer and Communication Engineering Technology*, édité par Hamzah Asyrani Sulaiman, Mohd Azlishah Othman, Mohd Fairuz Iskandar Othman, Yahaya Abd Rahim, et Naim Che Pee, 73-80. Lecture Notes in Electrical Engineering. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-24584-3_7.

Giura, P., et Wei Wang. 2012. « Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats ». *Science*. https://www.semanticscholar.org/paper/Using-Large-Scale-Distributed-Computing-to-Unveil-Giura-Wang/75e702d56a4a90f9c773a0e1fd0074cbe6910ead.

Giura, Paul, et Wei Wang. 2012. « A Context-Based Detection Framework for Advanced Persistent Threats ». In *2012 International Conference on Cyber Security*, 69-74. https://doi.org/10.1109/CyberSecurity.2012.16.

Greitzer, Frank L., et Deborah A. Frincke. 2010. « Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation ». In *Insider Threats in Cyber Security*, édité par Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, et Matt Bishop, 85-113. Advances in Information Security. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-7133-3_5.

Grow, Brian, Keith Epstein, et Chi-Chu Tschang. 2008. « The New E-spionage Threat ». *BusinessWeek*. https://web.archive.org/web/20110418080952/http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm.

Gu, Guofei, Roberto Perdisci, Junjie Zhang, et Wenke Lee. 2008. *BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection*. *CCS'08*.

Guerra-Manzanares, Alejandro, Sven Nõmm, et Hayretdin Bahsi. 2019. « Towards the Integration of a Post-Hoc Interpretation Step into the Machine Learning Workflow for IoT Botnet Detection ». In *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*, 1162-69. https://doi.org/10.1109/ICMLA.2019.00193.

Gulati, Radha. 2003. « The Threat of Social Engineering and Your Defense Against It | SANS Institute ». 2003. https://www.sans.org/white-papers/1232/.

Hachem, Nabil, Yosra Ben Mustapha, Gustavo Gonzalez Granadillo, et Herve Debar. 2011. « Botnets: Lifecycle and Taxonomy ». In *2011 Conference on Network and Information Systems Security*, 1-8. https://doi.org/10.1109/SAR-SSI.2011.5931395.

Haddadpajouh, Hamed, Ali Dehghantanha, Raouf Khayami, et Kim-Kwang Raymond Choo. 2018. « A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting ». *Future Generation Computer Systems* 85 (mars). https://doi.org/10.1016/j.future.2018.03.007.

Hamilton, S., W. L. Miller, Allen Ott, et O. S. Saydjari. 2002. « Challenges in Applying Game Theory to the Domain of Information Warfare † ». In . https://www.semanticscholar.org/paper/Challenges-in-Applying-Game-Theory-to-the-Domain-of-Hamilton-Miller/a65d0d3c8aae0f35a524c84d15748f85b01df7de.

Hartigan, John A. 1975. *Clustering Algorithms*. Wiley.

Hasan, Mahmudul, Md Islam, Ishrak Islam, et M.M.A. Hashem. 2019. « Attack and Anomaly Detection in IoT Sensors in IoT Sites Using Machine Learning Approaches », mai, 100059. https://doi.org/10.1016/j.iot.2019.100059.

Hassannataj Joloudari, Javad, Mojtaba Haderbadi, Amir Mashmool, Mohammad Ghasemigol, Shahab Shamshirband, et Amir Mosavi. 2020. « Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning ». *IEEE Access* 8 (octobre). https://doi.org/10.1109/ACCESS.2020.3029202.

Hejase, Ale, Hussin Hejase, et Jose Hejase. 2015. « Cyber Warfare Awareness in Lebanon: Exploratory Research ». *International Journal of Cyber-Security and Digital Forensics* Vol 4 (septembre):482-97. https://doi.org/10.17781/P001892.

Hejase, Hussin, Hasan Kazan, et Imad Moukadem. 2020. *Advanced Persistent Threats (APT): An Awareness Review*. https://doi.org/10.13140/RG.2.2.31300.65927.

Hinton, Geoffrey. 2009. « Deep belief networks ». *Scholarpedia* 4 (janvier):5947. https://doi.org/10.4249/scholarpedia.5947.

Hochreiter, Sepp, et Jürgen Schmidhuber. 1997. « Long Short-term Memory ». *Neural computation* 9 (décembre):1735-80. https://doi.org/10.1162/neco.1997.9.8.1735.

Hodge, Victoria J., et Jim Austin. 2004. « A Survey of Outlier Detection Methodologies ». *Artificial Intelligence Review* 22 (2): 85-126. https://doi.org/10.1007/s10462-004-4304-y.

Hofer-Schmitz, Katharina, Ulrike Kleb, et Branka Stojanović. 2021. « The Influences of Feature Sets on the Detection of Advanced Persistent Threats ». *Electronics* 10 (6): 704. https://doi.org/10.3390/electronics10060704.

Hofkirchner, Wolfgang, et Mark Burgin. 2017. *Future Information Society, The: Social And Technological Problems*. World Scientific.

Holland, Rick. 2013. « Introducing Forrester's Cyber Threat Intelligence Research ». 2013. https://web.archive.org/web/20140415054512/http://blogs.forrester.com/rick_holland/13-02-14-introducing_forresters_cyber_threat_intelligence_research.

Hudson, Barbara. 2013. « Advanced Persistent Threats: Detection, Protection and Prevention ». https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Sophos_Advanced_Persistent_Threats.pdf.

Huh, Jun, John Lyle, Cornelius Namiluko, et Andrew Martin. 2011. « Managing application whitelists in trusted distributed systems ». *Future Generation Comp. Syst.* 27 (février):211-26. https://doi.org/10.1016/j.future.2010.08.014.

Hutchins, Eric, Michael Cloppert, et Rohan Amin. 2011. « Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains ». *Leading Issues in Information Warfare & Security Research* 1 (janvier).

IC Espionage. 2010. « Shadows In The Cloud: Investigating Cyber Espionage 2.0 ». https://www.nartv.org/mirror/shadows-in-the-cloud.pdf.

ISACA. 2016. « Book Review: Advanced Persistent Threats ». ISACA. 2016. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/advanced-persistent-threats-how-to-manage-the-risk-to-your-business.

IT Governance. 2023. « Advanced Persistent Threats (APTs) ». 2023. https://itgovernance.co.uk/advanced-persistent-threats-apt.

Jeun, Inkyung, Youngsook Lee, et Dongho Won. 2012. « A Practical Study on Advanced Persistent Threats ». In *Computer Applications for Security, Control and System Engineering*, édité par Tai-hoon Kim, Adrian Stoica, Wai-chi Fang, Thanos Vasilakos, Javier García Villalba, Kirk P. Arnett, Muhammad Khurram Khan, et Byeong-Ho Kang,

144-52. Communications in Computer and Information Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-35264-5_21.

Jia, Bin, Zhaowen Lin, et Yan Ma. 2015. *Advanced Persistent Threat Detection Method Research Based on Relevant Algorithms to Artificial Immune System*. Vol. 520. https://doi.org/10.1007/978-3-662-47401-3_29.

Johnson, Ariana. 2016. « Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation ». *North Carolina Banking Institute* 20 (1): 277.

Johnson, John, et Emilie Hogan. 2013. *A graph analytic metric for mitigating advanced persistent threat*. Vol. 129. https://doi.org/10.1109/ISI.2013.6578801.

Kaspersky. 2015. « The Duqu 2.0 ». https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

———. 2023a. « Targeted Cyberattacks Logbook ». APT Kaspersky Securelist. 2023. https://apt.securelist.com.

———. 2023b. « What Is an Advanced Persistent Threat (APT)? » www.kaspersky.com. 19 avril 2023. https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.

Kaushik, Atul, Emmanuel Pilli, et R. Joshi. 2010. *Network Forensic System for Port Scanning Attack*. https://doi.org/10.1109/IADCC.2010.5422935.

Kholidy, Hisham A., Abdelkarim Erradi, Sherif Abdelwahed, et Abdulrahman Azab. 2014. « A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems ». *2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing*, août, 14-19. https://doi.org/10.1109/DASC.2014.12.

Kim, Hyunjoo, Jonghyun Kim, Ikkyun Kim, et Tai-myung Chung. 2015. « Behavior-based anomaly detection on big data ». *Australian Information Security Management Conference*, janvier. https://doi.org/10.4225/75/57b69d1ed938e.

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, et Edgar Weippl. 2015. « Advanced social engineering attacks ». *Journal of Information Security and Applications*, Special Issue on Security of Information and Networks, 22 (juin):113-22. https://doi.org/10.1016/j.jisa.2014.09.005.

Kyriakopoulos, Kostas, Francisco J. Aparicio-Navarro, Ibrahim Ghafir, Sangarapillai Lambotharan, et Jonathon Chambers. 2018. *Multi-stage attack detection using contextual information*. Loughborough University. https://doi.org/10.1109/MILCOM.2018.8599708'].

Langner, Ralph. 2011. « Stuxnet: Dissecting a Cyberwarfare Weapon ». *IEEE Security & Privacy* 9 (3): 49-51. https://doi.org/10.1109/MSP.2011.67.

Lee, Bernard, Manmeet (Mandy) Mahinderjit Singh, et Azizul Rahman Mohd Shariff. 2019. « APTGuard : Advanced Persistent Threat (APT) Detections and Predictions using Android Smartphone: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018 ». In , 545-55. https://doi.org/10.1007/978-981-13-2622-6_53.

Lee, Martin. 2011. « Clustering Disparate Attacks: Mapping The Activities of The Advanced Persistent Threat. » *21st Virus Bulletin International Conference*, octobre. https://www.academia.edu/2352875/CLUSTERING_DISPARATE_ATTACKS_MAPPING_THE_ACTIVITIES_OF_THE_ADVANCED_PERSISTENT_THREAT.

Lemay, Antoine, Joan Calvet, François Menet, et José M. Fernandez. 2018. « Survey of publicly available reports on advanced persistent threat actors ». *Computers & Security* 72 (janvier):26-59. https://doi.org/10.1016/j.cose.2017.08.005.

Lim, Joo, Shanton Chang, Sean Maynard, et Atif Ahmad. 2009. « Exploring the Relationship between Organizational Culture and Information Security Culture ». *Australian Information Security Management Conference*, décembre. https://doi.org/10.4225/75/57b4065130def.

Lin, Min, Qiang Chen, et Shuicheng Yan. 2013. « Network In Network ». *CoRR*, décembre. https://www.semanticscholar.org/paper/Network-In-Network-Lin-Chen/5e83ab70d0cbc003471e87ec306d27d9c80ecb16.

Liu, Yali, Cherita Corbett, Ken Chiang, Rennie Archibald, Biswanath Mukherjee, et Dipak Ghosal. 2009. *SIDD: A Framework for Detecting Sensitive Data Exfiltration by an Insider Attack*. *Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2009.390.

Lo, Chi-Chun, et Wan-Jia Chen. 2012. « A Hybrid Information Security Risk Assessment Procedure Considering Interdependences between Controls ». *Expert Systems with Applications* 39 (1): 247-57. https://doi.org/10.1016/j.eswa.2011.07.015.

Lockheed Martin. 2023. « Cyber Kill Chain® ». Lockheed Martin. 2023. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Mahadevan, Vijay, Wei-Xin LI, Viral Bhalodia, et Nuno Vasconcelos. 2010. *Anomaly Detection in Crowded Scenes*. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. https://doi.org/10.1109/CVPR.2010.5539872.

Maloney, Sarah. 2018. « What Is an Advanced Persistent Threat (APT)? » 2018. https://www.cybereason.com/blog/advanced-persistent-threat-apt.

Mandiant. 2013. « APT1 | Exposing One of China's Cyber Espionage Units ». Mandiant. 2013. https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units.

———. 2021. « Today's Top Cyber Trends & Attacks Insights | M-Trends 2021 ». Mandiant. 2021. https://www.mandiant.com/resources/reports/m-trends-2021.

Manhas, Jatinder, et Shallu Kotwal. 2021. « Implementation of Intrusion Detection System for Internet of Things Using Machine Learning Techniques ». In , édité par Kaiser J. Giri, Shabir Ahmad Parah, Rumaan Bashir, et Khan Muhammad, 217-37. Algorithms for Intelligent Systems. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-8711-5_11.

Marchetti, Mirco, Fabio Pierazzi, Michele Colajanni, et Alessandro Guido. 2016. « Analysis of high volumes of network traffic for Advanced Persistent Threat detection ». *Computer Networks* 109 (juin). https://doi.org/10.1016/j.comnet.2016.05.018.

Matthews, Tim. 2019. « Operation Aurora – 2010's Major Breach by Chinese Hackers ». Exabeam. 8 janvier 2019. https://www.exabeam.com/information-security/operation-aurora/.

McAfee. 2010a. « Protecting Your Critical Assets ». https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

———. 2010b. « Protecting Your Critical Assets - Lessons Learned from "Operation Aurora" ». https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

———. 2018. « The Economic Impact of Cybercrime No Slowing Down. » https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

McDermott, Christopher D., Farzan Majdani, et Andrei V. Petrovski. 2018. « Botnet Detection in the Internet of Things using Deep Learning Approaches ». In *2018 International Joint Conference on Neural Networks (IJCNN)*, 1-8. https://doi.org/10.1109/IJCNN.2018.8489489.

McHugh, John. 2000. « Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory ». *ACM Transactions on Information and System Security* 3 (4): 262-94. https://doi.org/10.1145/382912.382923.

McMahon, Dave, et Rafal Rohozinski. 2013. « The Dark Space Project: Defence R&D Canada – Centre for Security Science Contractor Report DRDC CSS CR 2013-007 ».

Merz, Terry. 2019. « A Context-Centred Research Approach to Phishing and Operational Technology in Industrial Control Systems | Journal of Information Warfare ». 2019. https://www.jinfowar.com/journal/volume-18-issue-4/context-centred-research-approach-phishing-operational-technology-industrial-control-systems.

Messier, Ric. 2013. *GSEC GIAC Security Essentials Certification All-in-One Exam Guide*. McGraw Hill Professional.

Microsoft. 2022. « Threats - Microsoft Threat Modeling Tool - Azure - STRIDE ». 25 août 2022. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

Milajerdi, Sadegh M., Rigel Gjomemo, Birhanu Eshete, R. Sekar, et V.N. Venkatakrishnan. 2019. « HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows ». In *2019 IEEE Symposium on Security and Privacy (SP)*, 1137-52. https://doi.org/10.1109/SP.2019.00026.

Mitnick, Kevin D., et William L. Simon. 2011. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

MITRE. 2021. « MiniDuke, Software S0051 | MITRE ATT&CK® ». 2021. https://attack.mitre.org/software/S0051/.

Montgomery, Douglas C., Elizabeth A. Peck, et G. Geoffrey Vining. 2012. *Introduction to Linear Regression Analysis*. John Wiley & Sons.

Moon, Daesung, Hyungjin Im, Jae Dong Lee, et Jong Hyuk Park. 2014. « MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats ». *Symmetry* 6 (4): 997-1010. https://doi.org/10.3390/sym6040997.

Muszyński, Józef, et Greg Shipley. 2008. « Narzędzia SIEM (Security Information and Event Management) ». Computerworld. 2008. https://www.computerworld.pl/news/Narzedzia-SIEM-Security-Information-and-Event-Management,325855.html.

Nance, Kara, et Matt Bishop. 2017. *Introduction to Deception, Digital Forensics, and Malware Minitrack*. https://doi.org/10.24251/HICSS.2017.731.

Nar, Kamil, et S. Shankar Sastry. 2018. « An Analytical Framework to Address the Data Exfiltration of Advanced Persistent Threats ». In *2018 IEEE Conference on Decision and Control (CDC)*, 867-73. https://doi.org/10.1109/CDC.2018.8619834.

Nicho, Mathew, et Christopher D. McDermott. 2019. « Dimensions of 'Socio' Vulnerabilities of Advanced Persistent Threats ». In *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 1-5. https://doi.org/10.23919/SOFTCOM.2019.8903788.

Nick. 2018. « Turla APT Group's Espionage Campaigns Now Employs Adobe Flash Installer and Ingenious Social Engineering ». *Cyber Defense Magazine* (blog). 16 janvier 2018. https://www.cyberdefensemagazine.com/turla-apt-groups-espionage-campaigns-now-employs-adobe-flash-installer-and-ingenious-social-engineering/.

Nissim, Nir, Aviad Cohen, Chanan Glezer, et Yuval Elovici. 2015. « Detection of Malicious PDF Files and Directions for Enhancements: A State-of-the Art Survey ». *Computers & Security* 48 (février):246-66. https://doi.org/10.1016/j.cose.2014.10.014.

NIST, Initiative Joint Task Force Transformation. 2011. « Managing Information Security Risk: Organization, Mission, and Information System View ». NIST Special Publication (SP) 800-39. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39.

Nunes, Eric, Ahmad Diab, Andrew Gunn, Ericsson Marin, Vineet Mishra, Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, et Paulo Shakarian. 2016. *Darknet and deepnet mining for proactive cybersecurity threat intelligence*. https://doi.org/10.1109/ISI.2016.7745435.

Oehmen, Christopher, Elena Peterson, et Scott Dowson. 2010. « An organic model for detecting cyber-events ». In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 1-4. CSIIRW '10. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1852666.1852740.

Paganini, Pierluigi. 2019. « Iran-Linked APT33 Updates Infrastructure Following Its Public Disclosure ». Security Affairs. 1 juillet 2019. https://securityaffairs.com/87784/apt/apt33-updates-infrastructure.html.

Park, Seong-Taek, Guozhong Li, et Jae-Chang Hong. 2020. « A Study on Smart Factory-Based Ambient Intelligence Context-Aware Intrusion Detection System Using Machine Learning ». *Journal of Ambient Intelligence and Humanized Computing* 11 (4): 1405-12. https://doi.org/10.1007/s12652-018-0998-6.

Parrish, Jr, James L., Janet L. Bailey, et James F. Courtney. 2009. « A Personality Based Model for Determining Susceptibility to Phishing Attacks ». http://www.swdsi.org/swdsi2009/papers/9J05.pdf.

Peikert, Chris. 2016. « A Decade of Lattice Cryptography ». *Foundations and Trends® in Theoretical Computer Science* 10 (4): 283-424. https://doi.org/10.1561/0400000074.

Pfleeger, Shari, Angela Sasse, et Adrian Furnham. 2014. « From Weakest Link to Security Hero: Transforming Staff Security Behavior ». *Journal of Homeland Security and Emergency Management* 11 (décembre). https://doi.org/10.1515/jhsem-2014-0035.

Probst, Philipp, Marvin N. Wright, et Anne-Laure Boulesteix. 2019. « Hyperparameters and Tuning Strategies for Random Forest ». *WIREs Data Mining and Knowledge Discovery* 9 (3): e1301. https://doi.org/10.1002/widm.1301.

PWC. 2014. « Managing cyber risks in an interconnected world ». https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Quintero-Bonilla, Santiago, et Angel Martín del Rey. 2020. « A New Proposal on the Advanced Persistent Threat: A Survey ». *Applied Sciences* 10 (11): 3874. https://doi.org/10.3390/app10113874.

Rachmadi, Salman, Satria Mandala, et Dita Oktaria. 2021. « Detection of DoS Attack using AdaBoost Algorithm on IoT System ». In *2021 International Conference on Data Science*

and Its Applications (ICoDSA), 28-33. https://doi.org/10.1109/ICoDSA53588.2021.9617545.

Radzikowski, Shem. 2015. « CyberSecurity: Origins of the Advanced Persistent Threat (APT) ». Dr.Shem. 8 octobre 2015. https://DrShem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/.

Rafique, M. Zubair, Ping Chen, Christophe Huygens, et Wouter Joosen. 2014. « Evolutionary algorithms for classification of malware families through different network behaviors ». In *Proceedings of the 2014 Annual Conference on Genetic and Evolutionary Computation*, 1167-74. GECCO '14. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2576768.2598238.

Rass, Stefan, Sandra König, et Stefan Schauer. 2017. « Defending Against Advanced Persistent Threats Using Game-Theory ». *PLOS ONE* 12 (1): e0168675. https://doi.org/10.1371/journal.pone.0168675.

Roldán, José, Juan Boubeta-Puig, José Luis Martínez, et Guadalupe Ortiz. 2020. « Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks ». *Expert Systems with Applications* 149 (juillet):113251. https://doi.org/10.1016/j.eswa.2020.113251.

Rot, Artur. 2009. « Enterprise Information Technology Security: Risk Management Perspective ». *Lecture Notes in Engineering and Computer Science* 2179 (octobre).

———. 2016. « Zarządzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki ». In , 35-50.

Rot, Artur, et Bogusław Olszewski. 2017. *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*. https://doi.org/10.15439/2017F488.

Rowe, Mark. 2013. « Advanced Persistent Threats: How to Manage the Risk to Your Business ». Professional Security. 11 octobre 2013. https://professionalsecurity.co.uk/reviews/advanced-persistent-threats-how-to-manage-the-risk-to-your-business/.

Russell, Chelsa. 2002. « Security Awareness - Implementing an Effective Strategy | SANS Institute ». 2002. https://www.sans.org/white-papers/418/.

SANS. 2013. « Assessing Outbound Traffic to Uncover Advanced Persistent Threat ». SANS Technology Institute.

Santoro, Diego, Gines Escudero-Andreu, Kostas Kyriakopoulos, Francisco J. Aparicio-Navarro, David J. Parish, et M. Vadursi. 2017. « A hybrid intrusion detection system for virtual jamming attacks on wireless networks », janvier, 79-87. https://doi.org/10.1016/j.measurement.2017.05.034'].

Sasaki, Takayuki. 2011. « Towards Detecting Suspicious Insiders by Triggering Digital Data Sealing ». In *2011 Third International Conference on Intelligent Networking and Collaborative Systems*, 637-42. Fukuoka, Japan: IEEE. https://doi.org/10.1109/INCoS.2011.157.

Schatz, Daniel, Rabih Bashroush, et Julie Wall. 2017. « Towards a More Representative Definition of Cyber Security ». *Journal of Digital Forensics, Security and Law* 12 (2). https://doi.org/10.15394/jdfsl.2017.1476.

Schmid, M., F. Hill, et A.K. Ghosh. 2002. « Protecting data from malicious software ». *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 199-208. https://doi.org/10.1109/CSAC.2002.1176291.

Schubert, Erich, Jörg Sander, Martin Ester, Hans Kriegel, et Xiaowei Xu. 2017. « DBSCAN revisited, revisited: Why and how you should (still) use DBSCAN ». *ACM Transactions on Database Systems* 42 (juillet):1-21. https://doi.org/10.1145/3068335.

SecureList. 2013. « “Red October” Diplomatic Cyber Attacks Investigation ». 14 janvier 2013. https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/.

Sexton, Joseph, Curtis Storlie, et Joshua Neil. 2015. « Attack Chain Detection ». *Statistical Analysis and Data Mining: The ASA Data Science Journal* 8 (5-6): 353-63. https://doi.org/10.1002/sam.11296.

Shalaginov, Andrii, Katrin Franke, et Xiongwei Huang. 2016. *Malware Beaconing Detection by Mining Large-scale DNS Logs for Targeted Attack Identification*.

Shamah, David. 2013. « Cyber Espionage Bug Attacking Middle East, but Israel Untouched — so Far ». 2013. http://www.timesofisrael.com/new-cyber-bug-targeting-middle-east-but-israel-untouched-so-far/.

Sharma, Pradip Kumar, Seo Yeon Moon, Daesung Moon, et Jong Hyuk Park. 2017. « DFA-AD: A Distributed Framework Architecture for the Detection of Advanced Persistent Threats ». *Cluster Computing* 20 (1): 597-609. https://doi.org/10.1007/s10586-016-0716-0.

Shenwen, Lin, Li Yingbo, et Du Xiongjie. 2015. « Study and research of APT detection technology based on big data processing architecture ». *2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*, mai, 313-16. https://doi.org/10.1109/ICEIEC.2015.7284547.

Shevchenko, Nataliya, Timothy A. Chick, Paige O’Riordan, et Thomas Patrick Scanlon. 2018. « Threat Modeling: A Summary of Available Methods ». https://apps.dtic.mil/sti/citations/AD1084024.

Shin, Seongjun, Seungmin Lee, Hyunwoo Kim, et Sehun Kim. 2013. « Advanced probabilistic approach for network intrusion forecasting and detection ». *Expert Systems with Applications* 40 (janvier):315-22. https://doi.org/10.1016/j.eswa.2012.07.057.

Shirey, Rob. 2000. « Internet Security Glossary ». Request for Comments RFC 2828. Internet Engineering Task Force. https://doi.org/10.17487/RFC2828.

Siddiqui, Sana, Salman Khan, K. Ferens, et Witold Kinsner. 2016. *Detecting Advanced Persistent Threats using Fractal Dimension based Machine Learning Classification*. https://doi.org/10.1145/2875475.2875484.

Sigholm, Johan, et Martin Bang. 2013. *Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats*. https://doi.org/10.1109/EISIC.2013.37.

SignalSense. 2015. « Using Deep Learning To Detect Threat, SignalSense, White Paper »,. https://www.ten-inc.com/presentations/deep_learning.pdf.

Sim, Kevin, Emma Hart, et Ben Paechter. 2014. « A Lifelong Learning Hyper-heuristic Method for Bin Packing ». *Evolutionary computation* 23 (février). https://doi.org/10.1162/EVCO_a_00121.

Singer, Peter W., et Allan Friedman. 2014. *Cybersecurity: What Everyone Needs to Know*. OUP USA.

Singh, Abhishek, et Zheng Bu. 2014. « Hot Knives Through Butter: Bypassing Automated Analysis Systems (Black Hat USA 2013) - InfoconDB ». 2014. https://infocondb.org/con/black-hat/black-hat-usa-2013/hot-knives-through-butter-bypassing-automated-analysis-systems.

Smart, Steven J. 2011. « Joint Targeting in Cyberspace ». https://apps.dtic.mil/sti/citations/ADA555785.

Soong, T. T. 2004. « Fundamentals of Probability and Statistics for Engineers | Wiley ». Wiley.Com. 2004. https://www.wiley.com/en-us/Fundamentals+of+Probability+and+Statistics+for+Engineers-p-9780470868157.

Sriram, S., R. Vinayakumar, Mamoun Alazab, et Soman KP. 2020. « Network Flow based IoT Botnet Attack Detection using Deep Learning ». In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 189-94. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162668.

Stevens, Tim. 2018. « Global Cybersecurity: New Directions in Theory and Methods ». *Politics and Governance* 6 (2): 1-4. https://doi.org/10.17645/pag.v6i2.1569.

Swisscom. 2019. « Report on the threat situation | SME | Swisscom ». 2019. https://www.swisscom.ch/en/business/sme/downloads/report-threat-situation-switzerland-2019.html.

Symantec. 2018a. « 2018 Internet Security Threat Report ». https://docs.broadcom.com/doc/istr-23-executive-summary-en.

———. 2018b. « Advanced Persistent Threats: A Symantec Perspective ». https://web.archive.org/web/20180508161501/https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

Taddeo, Mariarosaria. 2012. « An analysis for a just cyber warfare ». In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1-10. https://ieeexplore.ieee.org/document/6243976.

Tanaka, Yasuyuki, Mitsuaki Akiyama, et Atsuhiro Goto. 2017. « Analysis of malware download sites by focusing on time series variation of malware ». *Journal of Computational Science* 22 (septembre):301-13. https://doi.org/10.1016/j.jocs.2017.05.027.

Tankard, Colin. 2011. « Advanced Persistent threats and how to monitor and deter them ». *Network Security* 2011 (8): 16-19. https://doi.org/10.1016/S1353-4858(11)70086-1.

Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, et Ali A. Ghorbani. 2009. « A detailed analysis of the KDD CUP 99 data set ». In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1-6. https://doi.org/10.1109/CISDA.2009.5356528.

Tollefson, Rodika. 2020. « ICS/SCADA Malware Threats | Infosec ». 2020. https://resources.infosecinstitute.com/topics/scada-ics-security/ics-scada-malware-threats/.

Townsend, Kevin. 2018. « Knowing Value of Data Assets Is Crucial to Cybersecurity Risk Management ». SecurityWeek. 3 décembre 2018. https://www.securityweek.com/knowing-value-data-assets-crucial-cybersecurity-risk-management/.

Trend. 2012. « Spear-Phishing Email: Most Favored APT Attack Bait ». https://documents.trendmicro.com/assets/wp/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

Ussath, Martin, David Jaeger, Feng Cheng, et Christoph Meinel. 2016. « Advanced persistent threats: Behind the scenes ». *2016 Annual Conference on Information Science and Systems (CISS)*, mars, 181-86. https://doi.org/10.1109/CISS.2016.7460498.

Villeneuve, Nart, et James Bennett. 2012. « Detecting APT Activity with Network Traffic Analysis ». https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf.

Villeneuve, Nart, et James T. Bennett. 2014. « XtremeRAT: Nuisance or Threat? » Mandiant. 2014. https://www.mandiant.com/resources/blog/xtremerat-nuisance-or-threat.

Virvilis, Nikos, et Dimitris Gritzalis. 2013. « The Big Four - What We Did Wrong in Advanced Persistent Threat Detection? » In *2013 International Conference on Availability, Reliability and Security*, 248-54. https://doi.org/10.1109/ARES.2013.32.

Virvilis, Nikos, Dimitris Gritzalis, et Theodoros Apostolopoulos. 2013. « Trusted Computing vs. Advanced Persistent Threats: Can a Defender Win This Game? » In *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, 396-403. https://doi.org/10.1109/UIC-ATC.2013.80.

Vukalovic, J., et Damir Delija. 2015. *Advanced Persistent Threats - detection and defense*. https://doi.org/10.1109/MIPRO.2015.7160480.

Wahla, Arfan, Lan Chen, Yali Wang, Rong Chen, et Fan Wu. 2019. « Automatic Wireless Signal Classification in Multimedia Internet of Things: An Adaptive Boosting Enabled Approach ». *IEEE Access* PP (novembre):1-1. https://doi.org/10.1109/ACCESS.2019.2950989.

Wang, Xiali, et Xiang Lu. 2020. « A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices ». *Wireless Communications and Mobile Computing* 2020 (octobre):1-13. https://doi.org/10.1155/2020/8838571.

Wang, Xu, Kangfeng Zheng, Xinxin Niu, Bin Wu, et Chunhua Wu. 2016. « Detection of command and control in advanced persistent threat based on independent access ». In *2016 IEEE International Conference on Communications (ICC)*, 1-6. https://doi.org/10.1109/ICC.2016.7511197.

Wang, Yuan, Yongjun Wang, Jing Liu, et Zhijian Huang. 2014. « A Network Gene-Based Framework for Detecting Advanced Persistent Threats ». In *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 97-102. https://doi.org/10.1109/3PGCIC.2014.41.

Wang, Yuan, Yongjun Wang, Jing Liu, Zhijian Huang, et Peidai Xie. 2016. *A Survey of Game Theoretic Methods for Cyber Security*. https://doi.org/10.1109/DSC.2016.90.

Waqas, Muhammad, Kamlesh Kumar, Asif Ali Laghari, Umair Saeed, Muhammad Malook Rind, Aftab Ahmed Shaikh, Fahad Hussain, Athaul Rai, et Abdul Qayoom Qazi. 2022. « Botnet Attack Detection in Internet of Things Devices over Cloud Environment via Machine Learning ». *Concurrency and Computation: Practice and Experience* 34 (4): e6662. https://doi.org/10.1002/cpe.6662.

Wright, John, Yi Ma, Julien Mairal, Guillermo Sapiro, Thomas S. Huang, et Shuicheng Yan. 2010. « Sparse Representation for Computer Vision and Pattern Recognition ». *Proceedings of the IEEE* 98 (6): 1031-44. https://doi.org/10.1109/JPROC.2010.2044470.

Wu, Xindong, Vipin Kumar, J. Ross Quinlan, Joydeep Ghosh, Qiang Yang, Hiroshi Motoda, Geoffrey J. McLachlan, et al. 2008. « Top 10 Algorithms in Data Mining ». *Knowledge and Information Systems* 14 (1): 1-37. https://doi.org/10.1007/s10115-007-0114-2.

Xu, Lei, Chunxiao Jiang, Jian Wang, Yong Ren, Jian Yuan, et Mohsen Guizani. 2015. « Game theoretic data privacy preservation: Equilibrium and pricing ». In *2015 IEEE International Conference on Communications (ICC)*, 7071-76. https://doi.org/10.1109/ICC.2015.7249454.

Yadav, Sandeep, Ashwath Kumar Krishna Reddy, A. L. Narasimha Reddy, et Supranamaya Ranjan. 2012. « Detecting Algorithmically Generated Domain-Flux Attacks With DNS

Traffic Analysis ». *IEEE/ACM Transactions on Networking* 20 (5): 1663-77. https://doi.org/10.1109/TNET.2012.2184552.

Yan, Xiaohuan, et J. Zhang. 2013. « A Early Detection of Cyber Security Threats using Structured Behavior Modeling ». In . https://www.semanticscholar.org/paper/A-Early-Detection-of-Cyber-Security-Threats-using-Yan-Zhang/92b0c21afbf1941cb27e707c50e51bd76a8b1d45.

Yang, Lu Xing, Pengdeng Li, Xiaofan Yang, et Yuan Yan Tang. 2017. « Security Evaluation of the Cyber Networks under Advanced Persistent Threats ». *IEEE Access* 5 (8053761): 20111-23. https://doi.org/10.1109/ACCESS.2017.2757944.

Yasar, Kinza, et Linda Rosencrance. 2021. « What Is an Advanced Persistent Threat (APT)? | Definition from TechTarget ». Security. 2021. https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT.

Zhang, Chongzhen, Yanli Chen, Yang Meng, Fangming Ruan, Runze Chen, Yidan Li, et Yaru Yang. 2021. « A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques ». Édité par Savio Sciancalepore. *Security and Communication Networks* 2021 (janvier):1-15. https://doi.org/10.1155/2021/6610675.

Zhang, Ru, Yanyu Huo, Jianyi Liu, et Fangyu Weng. 2017. « Constructing APT Attack Scenarios Based on Intrusion Kill Chain and Fuzzy Clustering ». *Security and Communication Networks* 2017 (décembre):e7536381. https://doi.org/10.1155/2017/7536381.

Zimba, Aaron, Hongsong Chen, Zhaoshun Wang, et Mumbi Chishimba. 2020. « Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics ». *Future Generation Computer Systems* 106 (mai):501-17. https://doi.org/10.1016/j.future.2020.01.032.

Zions Bancorporation. 2012. « A Case Study In Security Big Data Analysis ». 2012. https://www.darkreading.com/cybersecurity-analytics/a-case-study-in-security-big-data-analysis.

Zou, Qingtian, Xiaoyan Sun, Peng Liu, et Anoop Singhal. 2020. « An Approach for Detection of Advanced Persistent Threat Attacks », nº 12 (décembre), 92-26. https://doi.org/10.1109/MC.2020.3021548.